Mr. John Mott-Smith
Director of Voting Systems
Office of the Secretary of State
1500 11th Street
Sacramento CA 95814

7 Sep 04

Subject: Addendum to Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19 for AccuVote Optical Scan (AV-OS) Central Count Voting System, Firmware Version. 2.0.1.2. with optional Accu-Feed Unit.

Executive Summary

State certification testing was conducted 1-2 Sep 2004, at the California Secretary of State Election Division offices in Sacramento, CA, to certify the AccuVote Optical Scan (AV-OS), Central Count Voting System with the new GEMS 1.18.19. The AV-OS, for both version 1.94W and 1.96.4 was tested for certification in July 2004 for operation under GEMS 1.18.19. The configuration for this test uses the same hardware but with a different firmware chip and exercises a section of GEMS 1.18.19 that has not been previously exercised.

This testing is for central count operations which, with multiple networked ballot counters, transfer the individual ballot records to the GEMS directly and then GEMS performs the tally operation. The Accu-Feed, an optional unit that fits over an AV-OS and permits the automatic feeding of paper ballots, was also included in this testing.

The testing for this version configuration showed equivalent level of compliance with the California Election Code. Prior reports of security weaknesses still largely apply with minor differences due to the altered process flow.

References:

1. [SVF0624] Freeman, *Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19, Key Card Tool Rev 1.0.1 , Voter Card Encoders (VCE) Rev 1.3.2, and AccuVote Touch Screen DRE (AV-TS R6), Firmware 4.3.15D*, 24 Jun 2004

2. [SVF0719] Freeman, *Addendum to Certification of the Diebold Election Systems Global Election Management Systems (GEMS) Version 1.18.19 for AccuVote Optical Scan (AV-OS) Precinct Counter, Version 1.64W and 1.96.4.*, 19 Jul 2004.

3. [GEMS-U] Diebold, *GEMS 1.18 User's Guide*, Rev 9.0, 13 Feb 2004

4. [CA OS Proc] Diebold, *State Of California Procedures Required For Use Of The AccuVote-OS Optical Scan Voting System*, Sep 2002

5. [Ciber1] Ciber Ltr, *Functional Testing of GEMS Version 1-18-19 with Central Count OS* , 31 Aug 2004

6. [Ciber2] Ciber Ltr, *Functional Testing of GEMS Version 1-18-19 with Central Count OS Functional Testing of GEMS Version 1-18-19 with VCProgrammer*, 7 Sep 2004

7. [0SCC] Diebold Document, *AccuVote-OS Central 2.0 Count User's Guide*, Rev 3.0 7 May 2004

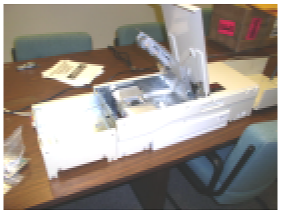
Introduction

In compliance with California Elections Code 19200 and 19205, Diebold Election Systems applied for certification for the following revisions:

a. AV-OS Central Count (AV-OSCC), Firmware Version 2.0.1.2 with GEMS 1.18.19

The AV-Optical Scan Ballot Counter (AV-OS) Firmware Versions 1.64W and 1.96.4 are certified in California under GEMS 1.18.19. The AV-OSCC variation adds a capability for performing the central count of absentee and paper provisional ballots using TCP/IP networked units.

The Accu-Feed unit shown below was also used in this test on one of two AV-OS central count units. The Accu-Feed is a powered ballot feeder that allows stacks of ballots to be placed in an input hopper and automatically feed the ballots to a AV-OS unit which it partially covers. The scanned ballot is then picked and moved into an output bopper w



The Accu-Feed has no vote processing function; testing objectives were limited to watching for ballot feed issues and valid responses to ballot sort/rejection signals from GEMS. The AV-OSCC firmware provides instructions only to move a single ballot through the scanner, capture the ballot image (both sides), and forward the image to GEMS Central Count Server. No ballot interpretation or data retention such as logs takes place on the Central Count device.

The AV-OSCC modification does not use the .abo files which were an issue in the last report [SVF0624].

NASED Qualifications

1. NASED Qualification: dated 5/20/04, N-1-06-12-12-002 (1990) includes:
   a. GEMS 1.18.19.
   b. AV-OS 1.94W.
   c. AV-OS 1.96.4.
   d. Others reported in [SVF0624].
2. [Ciber1] and [Ciber2] are letters reporting that the functional testing is completed. At the time of this report, the final ITA reports have not been finished.
3. The Accu-Feed has been inspected by the Hardware ITA who determined no Federal testing is needed.

Test Report Results

The same Primary test election used in prior tests was used again. The test election based on San Diego 2002 Primary uses seven political parties. Three parties, American Independent, Democratic, and Republican, were defined as allowing DTS voter participation and reporting with the Republican DTS not permitting participation in Presidential nominations. For this test, a backup copy of the election used in the prior GEMS 1.18.19 test for the AV-TS R6 and AV-OS was loaded and reset to use the AV-OSCC testing..

Security Access Controls

Previously identified security issues still apply to this configuration.

The AV-OSCC uses the same Key Card Tool as the AV-OS, AV-TS R6, and VCE. The direct connection between the networked AV-OSCC units and the GEMS central count server is nearly identical to the design of the SSL type upload link from AV-TS R6 DREs to GEMS. The only significant difference is that the records transmitted are scanned images which Diebold claims is similar to encryption in complexity.

During setup of the AV-OSCC, the IP Address of the GEMS central count server must be determined and programmed into AV-OSCC. This process involves a visible confirmation of the IP Address in the supervisor's window and a copy of the address is printed on the paper tape audit log on the AV-OSCC.

Since no records of ballots or vote counts is retained in memory, the security of the AV-OSCC after the ballot counting is a less severe requirement but tamperproof seals and/or locks should still be used prior and during counting to safeguard the operation from denial of service types of attack.

Conclusion

The testing for this version configuration showed equivalent level of compliance with the California Election Code. Prior reports of security weaknesses still largely apply with minor differences due to the altered process flow.

Sincerely,

Steven V. Freeman

Attachment:

List of the test configuration component

Attachment A.

Test Configuration Inventory

1. Dell Power Edge 600SC, HH18021 Chassis S/N
    a. 1.8 gigahertz, Pentium 4 processor
    b. 1 MByte RAM
    c. 20 GByte IDE Internal Hard Drive
    d. PLEXTOR CD-R PX-W1210S SCSI CdRom Drive
    e. 3.5 Diskette Drive
    f. ARCHIVE Python 06408-XXX SCSI Sequential Tape Drive (not used)
    g. Digi AccelePort Xem-PCI bus card
2. DigiPorts 8/EM, PC/8em DB25, S/N: (S) V 21488435. Port 1 (COM3) and 2 (COM4)
3. Hewitt Packard Laser 1200 Printer.
4. Hayes Accura Modem External V.92 for PC-US, P/N: H08-163286, S/N 1-84-H08-15328-C1-0009 (test only)
    (Normal installed version is U.S. Robotics Sportster)
5. Commercial-Off-The-Shelf Software
    a. MS Windows 2000 Server, Service Pack 4 (Build 2195) w additional patches for SP5.
        i. Window Internet Explorer 6.00.2800.1106
    b. Adobe Acrobat Version 6.0.0.2003051900
    c. Nero CD/DVD Rom Burning Suite, Version 6,
    d. WinZip 8.1, SR1
    e.
6. Auxiliary Equipment: AccuFeeder SN 50564 (optical connect)
7. Voting MachineUnit(s)
    a. AV-TS R6, 156996 BS 4.3.15.D
        i. Boot Loader 1.0.2
        ii. C/E Aug 8, 2002

    b. AV-OS 79811-04 30791, CC Firmware Ver. 2.0.1.2
    c. AV-OS 79811-04 30542, CC Firmware Ver. 2.0.1.2